REMARKS

Claim Objections

Claims 13 and 14 have been amended in the manner suggested by the examiner, thereby removing the basis for objection to these claims. Withdrawal of the objections to claims 13 and 14, accordingly, is respectfully requested.

Amendments to Claims

Claim 1 has been amended to clarify the intended meaning of the claim without affecting the scope of the claim as previously presented. The difference in quality of the user authentication specifically is clarified by denoting that the quality may be inherently a relatively lower quality or inherently a relatively higher quality from a security perspective. Support for the amendment is found on page 5, last paragraph wherein the terms "low-quality" and "higher-quality" are used to describe two authentication methods. The word "inherently" has been added for clarification to indicate that the method itself inherently provides less security or more security depending on the nature of the method (e.g., biometric versus PIN). The objective of the amendment is to better define the inherent nature of the user authentication method from a security perspective.

Claim 10 has been amended so that it is consistent with claim 1.

Claims 10 and 13 have been amended so they are consistent with amended claim 1.

Amendment to the Specification

The specification has been amended so that the language thereof is consistent with the language of the amended claims.

Claim Rejections – 35 USC §103

It is respectfully submitted that the examiner's reasoning with regard to the rejection of claims 1, 3-8, 10, 12 and 14 as reciting subject matter considered to be obvious in view of Mimura as modified by Kao is legally flawed. Mimura pure and simple requires a two step authentication procedure involving first a fingerprint verification of the user and thereafter an electronic authentication using a secret key that has been activated upon the fingerprint information submitted by the user matching fingerprint information stored in the system memory.

The examiner equates the Mimura system with the system recited in claim 1 of this application with the exception of teaching that the user may use one of different authentication methods to authenticate the user. In the first place, Mimura fails to disclose or teach a method for securing an electronic transaction wherein the quality of the transaction used is determined and then information about the authentication quality is attached to the result of the security-establishing operation. Mimura simply is concerned with a two stage authentication procedure involving first a fingerprint matching process followed by the typical electronic signature authentication process, wherein the second procedure is authorized only upon the user passing the first authentication test. There simply is no disclosure, suggestion or teaching in any form that information about the quality of the method used for authentication in accordance with Mimura may be attached to the result of a security establishing operation. Accordingly, at the very outset the examiner has failed to establish a *prima facie* basis for rejecting the claims on grounds of obviousness due to a significant missing element in the basic reference Mimura.

Recognizing that Mimura fails to specifically disclose that the user may use one of different user authentication methods for authentication, the examiner contends that a person skilled in the art would recognize from Kao that a user may use one of different user authentication methods to authenticate a user. The examiner concludes from this that the skilled person could readily modify the Mimura system by providing the user with the opportunity to use one of different user authentication methods to authenticate the user. The critical factor not explained by the examiner is that if Mimura is modified in the manner suggested by the examiner, the Mimura system would be defeated!

Specifically, Mimura requires a two step authentication procedure involving first a fingerprint matching process followed by an electronic signature process, wherein the electronic signature process is not authorized unless and until the fingerprint procedure reveals that the user is authenticated based on a biometric measurement.

Mimura is clear that both a biometric measurement procedure and an electronic signature or key procedure is required in accordance with the security system of Mimura.

If Mimura is modified in accordance with Kao so that only one or another security identification system is used, then the two step process of Mimura is defeated and it will not function for its intended purpose, namely a two stage security authentication process.

A careful reading of Kao reveals that it is intended to provide two or more independent authentication modes depending on the authentication procedure demanded by

the party to be accessed. In accordance with the examples given in Kao, such parties would be a bank and a broker. The system of Kao recognizes which client is to be accessed and adapts the GUI of the user's computer to reflect which program based on the client to be accessed is in use. The user then proceeds to obtain authentication and access to the client's computer after satisfying the authentication requirements of the specific client being accessed.

For example, if the client is a bank, a smart card authentication may be required and the GUI is adapted for such a procedure, prompting the user to enter the data required for the smart card authentication.

For a different client, such as a brokerage house, a user/password authentication may be required, wherein different modes of operation, i.e., a biometric fingerprint authentication, may be required.

The important consideration here is that in accordance with Kao, a user simply attempts to contact a client such as a bank or a brokerage house, and thereafter the system prompts the user to authenticate himself/herself using whichever authentication procedure is required by the client's program. No weight whatsoever is given to the authentication procedure in accordance with Kao, and further in accordance with Kao, no information regarding the quality of the authentication is attached to the result of the security establishing operation. Simply put, there is nothing in Kao to suggest that any of the client programs (i.e., bank, brokerage house, etc.) cares one whit about the quality of the authentication information apart from the fact that the user must satisfy the authentication procedure imposed by the client program.

Accordingly, the examiner's suggestion that Mimura in view of Kao results in a method corresponding to the rejected claims is legally defective and fails to establish a *prima facie* basis of obviousness due to fundamental missing elements in both Mimura and Kao. Both Mimura and Kao fail to suggest to a skilled person that the quality of authentication information may be attached to the result of a security-establishing operation, and furthermore modification of Mimura in accordance with the teachings of Kao would virtually defeat Mimura for its intended purpose, a result that entirely contradicts the proposition that a person skilled in the art would be motivated to modify Mimura in accordance with Kao to arrive at a process which the examiner equates with the rejected claims.

It is important for the examiner to understand that the method recited in claim 1, as described in the written description of this application, provides many advantages over prior

art authentication methods due to the fact that the recipient of the security message following authentication receives through the quality information contained in the message a statement on the quality of the authentication performed by the user (page 8, last paragraph). For example, quality information is joined firmly with a created digital signature to form a security message expediently within the secure messaging mechanism using the previously negotiated session keys. (Page 8, third full paragraph.) This system enables the user to use both lower quality and higher quality authentication procedures and as an additional important feature, attaches information about the quality of the authentication procedure with the results of the security establishing operation.

None of the prior art shows or teaches the methods recited in the rejected claims and withdrawal of the rejection of claims 1, 3-8, 10, 12 and 14 under 35 USC §103(a) as being unpatentable over Mimura in view of Kao is appropriate and the same is respectfully requested.

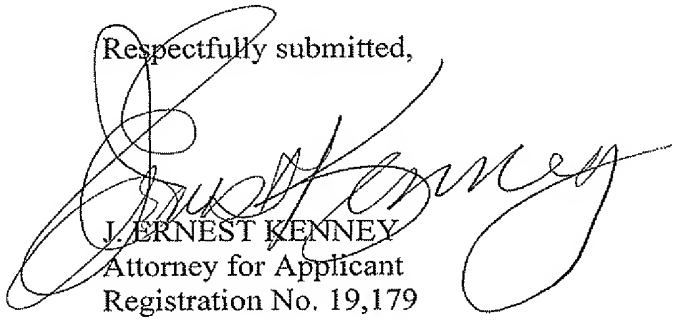
It is respectfully submitted that entry of the proposed amendments is appropriate under 37 CFR 1.116, as the amendments do not raise any further issues or require further searching by the examiner, moreover, the amendments are responsive to the new grounds for rejection expressed in the Action. Finally, the legal deficiency of the final rejection of claims 1, 3-8, 10, 12 and 14 as expressed above warrants withdrawal of the rejection of these claims on the grounds contended by the examiner.

With regard to claims 2, 9, 11 and 13, these claims are patentable at least on the basis of claims 1 and 10 from which they depend.

In the event that the examiner maintains the final rejection of the claims of this application, entry of the amendments for purposes of appeal is respectfully requested.

BACON & THOMAS, PLLC
625 Slaters Lane, 4th Floor
Alexandria, VA 22314-1176
Phone: (703) 683-0500
Facsimile: (703) 683-1080
Date: May 18, 2009

Respectfully submitted,



J. ERNEST KENNEY
Attorney for Applicant
Registration No. 19,179